PEATRIGG
Charitable Foundation

GDPR Policy

GDPR Policy for Peat Rigg Charitable Foundation

Introduction

Peat Rigg Charitable Foundation (referred to as "the Foundation") is committed to protecting the privacy and security of personal data. This policy outlines our approach to ensuring compliance with the General Data Protection Regulation (GDPR) and demonstrates our commitment to data protection.

Scope

This policy applies to all employees, volunteers, trustees, contractors, and partners who handle personal data on behalf of the Foundation. It covers all personal data processed by the Foundation, including data related to young people, SEND students, vulnerable adults, employees, and other stakeholders.

Data Protection Principles

The Foundation adheres to the following principles when processing personal data:

1. **Lawfulness, Fairness, and Transparency**: Personal data shall be processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation**: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation**: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date.
5. **Storage Limitation**: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and Confidentiality**: Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability**: The Foundation shall be responsible for, and be able to demonstrate compliance with, the GDPR principles.

Legal Basis for Processing

The Foundation processes personal data based on one or more of the following legal bases:

- Consent: Where appropriate, we obtain explicit consent from individuals to process their personal data.
- Contractual Necessity: Processing is necessary for the performance of a contract to which the data subject is a party.
- Legal Obligation: Processing is necessary for compliance with a legal obligation to which the Foundation is subject.
- Vital Interests: Processing is necessary to protect the vital interests of the data subject or another person.
- Legitimate Interests: Processing is necessary for the purposes of the legitimate interests pursued by the Foundation or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Data Subject Rights

Data subjects have the following rights under the GDPR:

- **Right to Access**: Individuals have the right to access their personal data and obtain information about how it is being processed.
- **Right to Rectification**: Individuals have the right to request the correction of inaccurate personal data.
- **Right to Erasure**: Individuals have the right to request the deletion of their personal data in certain circumstances.
- **Right to Restrict Processing**: Individuals have the right to request the restriction of processing of their personal data in certain circumstances.
- **Right to Data Portability**: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to request the transfer of that data to another controller.
- **Right to Object**: Individuals have the right to object to the processing of their personal data in certain circumstances.
- **Rights in Relation to Automated Decision-Making and Profiling**: Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significant effects.

Data Security

The Foundation implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- Encryption of personal data where appropriate.
- Regular assessment and evaluation of the effectiveness of security measures.
- Access controls to limit access to personal data to authorised individuals.
- Regular data protection training for staff and volunteers.

Data Breach Management

In the event of a data breach, the Foundation will:

1. Notify the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.
2. Communicate the breach to affected data subjects without undue delay if it is likely to result in a high risk to their rights and freedoms.
3. Take appropriate steps to mitigate the effects of the breach and prevent future occurrences.
4. Peat Rigg CIO's Data breach risk assessment sets out the mitigation measures taken by Peat Rigg to manage this risk.

Data Protection Officer

The Foundation has appointed a Data Protection Officer (DPO) who is responsible for overseeing data protection matters. The DPO can be contacted at:

- Name: Ian Thorpe
- Email: ian@peatrigg.org
- Phone: 01751 417112

Complaints

Individuals who wish to make a complaint about how their personal data is being processed by the Foundation or how a complaint has been handled can contact the DPO. If they are not satisfied with the response, they have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Review and Updates

This policy is reviewed annually and updated as necessary to ensure ongoing compliance with data protection laws. The latest version of this policy will always be available on Peat Rigg's website and upon request.

Contact Information

For any questions or concerns regarding this policy or data protection practices, please contact:

- Peat Rigg Charitable Foundation
- Address: Peat Rigg Outdoor Centre, Cropton, Pickering, North Yorkshire. YO18 8EX
- Email: info@peatrigg.org
- Phone: 01751 417112

A brief overview of the practical application of the use of data at Peat Rigg

- Personal details for individuals attending a course (contact details, medical, dietary information, any specific information that the booking contact within the organisation thinks it is appropriate for us to see). This information is destroyed at the end of your course.

- Contact information for the key people within organisations that use Peat Rigg, and other individuals and organisations that we work with: This is very basic information (name, work address, work phone and e mail details). We hold this information securely at Peat Rigg and endeavour to keep it accurate and up to date.

- Contact information for the (small number of) key people within organisations that no-longer use Peat Rigg: This is the same basic information as above. If you think you may be on this list, and want to be removed, please contact us and we would be more than happy to oblige.

- Details about individuals that have been involved in an accident or incident: We record the details of the accident or incident and basic details of the individual. These details will be kept securely at Peat Rigg for 7 years and destroyed thereafter.

- Personal details and records of Peat Rigg staff members, used for the lawful operations of Peat Rigg CIO. This will only be shared with organisations that have a right to see it and will comply with all points below.

- Photographs, images, and recordings of individuals will only be used strictly in accordance with the agreement that we have with each individual organisation.

We will only use your details for the above purposes.
These details will be kept securely.
We will not pass these details on to anybody else.
We will comply with every element of the GDPR regulations.